Enhanced delegated computing using coherence

Stefanie Barz[1], Vedran Dunjko[2,3], Florian Schlederer[1], Merritt Moore[1], Elham Kashefi[4], Ian A. Walmsley[1]
[1] *Clarendon Laboratory, Department of Physics, University of Oxford, OX1 3PU, United Kingdom,*
[2] *Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstrasse 21a, A-6020 Innsbruck, Austria*
[3] *Institute for Theoretical Physics, University of Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria*
[4] *School of Informatics, Informatics Forum, 10 Crichton Street, Edinburgh, EH8 9AB, UK*

A long-standing question is whether it is possible to delegate computational tasks securely. Recently, both a classical and a quantum solution to this problem were found [1, 2]. Here, we study the interplay of classical and quantum approaches and show how coherence can be used as a tool for secure delegated classical computation. We show that a client with limited computational capacity—restricted to an XOR gate—can perform universal classical computation by manipulating information carriers that may occupy superpositions of two states. Using single photonic qubits or coherent light, we experimentally implement secure delegated classical computations between an independent client and a server. The server has access to the light sources and measurement devices, whereas the client may use only a restricted set of passive optical devices to manipulate the light beams. Thus, our work highlights how minimal quantum and classical resources can be combined and exploited for classical computing.

INTRODUCTION

Cloud computing, the storage and processing of data on remote servers, has become highly relevant to modern information processing. The question of whether it is possible to compute over encrypted data was first asked some 35 years ago [3]. With the progress from stand-alone machines to large connected networks, the security of delegated computations has become increasingly important. In 2009, a classical algorithm, the fully homomorphic encryption protocol, was invented which provides computation security in data processing at remote servers [1]. At the same time, a quantum computing protocol was found which allows an almost-classical client to delegate a quantum computation securely to a quantum server [2, 4]. In contrast to the classical algorithm, the quantum version provides unconditional security [2, 5–7]; however, it requires classical communication of the order of the size of the computation. The trade-off between the amount of communication required and the desired security level is what motivates evaluation of a hybrid quantum-classical scheme [8].

Here, we study the interplay between classical and quantum delegated computation. The central question is what kind of additional resources a client, with capability restricted only to parity computations (XOR), needs in order to perform universal classical computations and to delegate those securely to a server. We show that this can be accomplished using *cobits*, systems capable of being in a coherent superposition of two "states" (see Fig. 1), for example single photonic qubits or coherent laser beams.

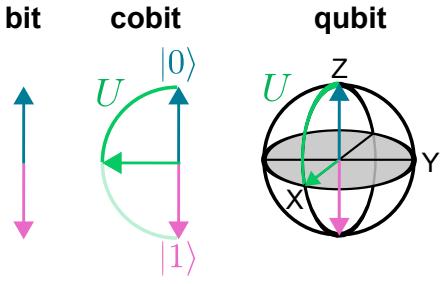

FIG. 1: Bit, cobits, and qubits. The bit is a two-level classical system, cobits are systems capable of being in a coherent superposition of two "states", and qubits are quantum systems. The operation U transforms basis states into superposition states and vice versa.

In our scheme, the server has access to cobits, and the client is restricted to parity computations and the local manipulation of the cobits. The protocol works in the following manner: the server sends cobits, and the client applies simple operations to them, dependent on some classical bits. The cobits are then sent back to the server, which performs a measurement. The result of the measurement depends on the client's manipulations and contains the encrypted outcome of the NAND operation on the client's classical bits. This means that the cobit enables the client to compute problems beyond her own power, since the NAND gate is universal for classical computation.

Further, we experimentally implement classical secure delegated computation by using single qubits or coherent laser beams as cobits. In our implementation, the client and the server are set up in two different laboratories, separated by more than 50 meters, and connected by optical fibres. Photonic systems are ideally suited for this task, since they can be easily manipulated and transmitted over large distances; however our scheme can be implemented using every physical system that provides coherence.

Note that the protocol and the implementation are classical in the sense of classical physics: they use purely classical means, effects and devices, including classical coherence. We note that this definition differs from the definition of "classical" in computer science, which is limited to only classical two-level bits and gates on these bits. Thus, our work also highlights the two different notions of classicality in physics and computer science.

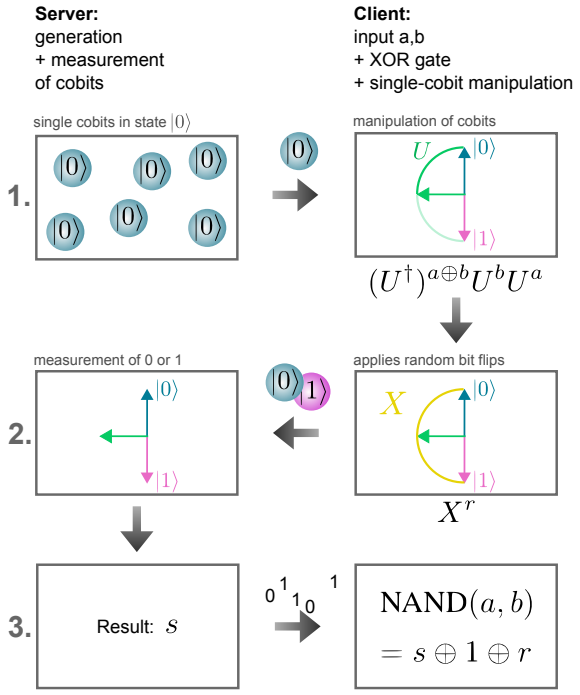

FIG. 2: Scheme of delegated NAND gate. The steps of the protocol are in detail described in the main text.

THEORY

Our work is based on a protocol for secure delegated classical computation using quantum resources [9]. It was shown that manipulations of only two-level bits are not sufficient for this task. Here, we reformulate the original work [9] and show that in the same setting adding classical coherence enables us to perform secure delegated classical computations.

The protocol is based on the implementation of a NAND gate using only parity computations and coherence. Here, we first describe the protocol using single cobits and show later its implementation with single photonic qubits and coherent beams, which relaxes the requirements of the initial theory [9]. In detail, the protocol works as explained in the following (see also Fig 2). First, the server generates cobits in the state $|0\rangle$ and sends these cobits to the client. The client wants to implement a NAND gate on two input bits a and b. The client encodes the result of a NAND(a,b) gate in the output cobit by applying the gate sequence:

$$|\text{NAND}(a,b)\oplus 1\rangle = (U^\dagger)^{a\oplus b}U^bU^a|0\rangle. \quad (1)$$

Here, U is an operation which brings the state $|0\rangle$ into a superposition of $|0\rangle$ and $|1\rangle$. If U is applied to the superposition of $|0\rangle$ and $|1\rangle$, the cobit will be in state $|1\rangle$ after the operation $(U(U|0\rangle) = |1\rangle)$. In our protocol, the operation U is or is not applied, depending on the values of a and b. Only if $a = b = 1$, the output cobit is in state $|1\rangle$, for all other settings of a and b, the output cobit is in state $|0\rangle$. Thus, the output cobit can be written as $|\text{NAND}(a,b)\oplus 1\rangle$ and effectively contains a NAND gate.

In order to hide the state of the output cobit to achieve secure delegated computing, the client applies an additional random bit flip X:

$$|\text{NAND}(a,b)\oplus 1\oplus r\rangle = X^r|\text{NAND}(a,b)\oplus 1\rangle, \quad (2)$$

where r is a random value.

The cobit is then sent back to the server, where a measurement in the $|0/1\rangle$ basis is performed. The result of this measurement, s, is returned to the client, who finally obtains the result NAND(a,b) by computing:

$$\text{NAND}(a,b) = s\oplus 1\oplus r. \quad (3)$$

A single classical bit is not sufficient to implement a NAND gate, because at least two bits are required. Our protocol shows that systems allowing for a coherent superposition of two states are sufficient. A single qubit also accomplishes this task in the fully quantum case. Here, the operation $U = R_y(\pi/2)$ is a rotation of $\pi/2$ around the Y axis of the Bloch sphere: $R_y(\theta) = \exp(-i\theta/2\sigma_y)$, σ_y is the Pauli operator, and the bit flip $X = \sigma_X$ is given by the Pauli operator . However, no quantum behavior is required in our setting. Every system that provides coherence can be used to implement our protocol.

Optics facilitates transmission of information between the server and the client and back. Experimentally, we make use of single photonic qubits or a coherent laser beam, since the logical states $|0\rangle$ and $|1\rangle$ can be encoded in the photon's or beam's polarization. The only difference is that when using a coherent state light beam multiple photons pass through the client's gates with the same settings. Since the security effectively reduces to a classical information-theoretical encryption (effectively a one-time pad) and is not relying on quantum properties vital in most of quantum cryptography (e.g. the no-cloning result for quantum states), having multiple copies of the same state does not reduce the security (see proof in SI).

The challenge when single qubits are used for the protocol is that probabilistic generation and optical losses affect the robustness of the protocol. Since the client is only capable of performing parity computations and the preparation of random bits, she cannot check whether the computation is correct or not. If the server does not send a photon or the photon gets lost, then the server fails to register a result. The easiest solution would be to send an additional classical bit on a different channel from the server to the client, which indicates that the procedure has worked. Dependent on the classical bit, the client could then repeat the computation. However, this is not possible in our framework as this routine would be equivalent to implementing a NAND gate and thus is beyond the client's capabilities. Using a laser beam for the implementation of the protocol has the advantage of providing robustness against these photon losses.

A NAND computation without considering the security aspects, was first proposed in another work [10]. There, a classical parity computer controlled three-qubit Greenberger-Horne-Zeilinger states in order to perform universal classical

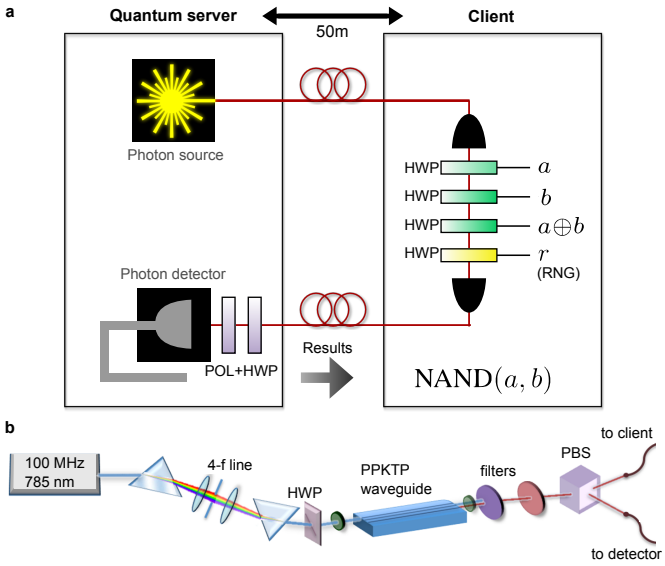

FIG. 3: Experimental setup. a. Setup of separated client and server. The server in "lab 1" generates and measures polarization-encoded single qubits or the polarization of an attenuated laser beam. The client in "lab 2" manipulates the polarization and encodes the NAND gate. b. Source for the generation of heralded single photons.

computation. This setting can be seen as a measurement-based version of ours—a rotation is performed via single-qubit measurements [11, 12]. Our work shows that the same functionality can be achieved without having any quantum resources at all. Furthermore, we achieve secure delegated computations by sending cobits. This reduction to the manipulation of "simple" resources, compared to the generation of entanglement, clearly decreases the experimental requirements and enables one to perform secure and delegated classical computations with minimal resources.

EXPERIMENTS

We implement the server and the client using two independent experimental setups running in two different laboratories, which are separated by 50 m (see Fig. 3).

We either use a heralded single photon source or a weak coherent laser beam for the implementation of the protocol. For both cases, we encode the states $|0\rangle$ and $|1\rangle$ in polarization, denoting horizontal and vertical polarization, respectively.

The heralded single photons are produced by type-II parametric down conversion in a Potassium Titanium Oxide Phosphate (KTP) crystal that has periodically poled waveguides [13]. A mode-locked fiber-based femtosecond laser produces 90 fs long pulses at 1575 nm with a repetition rate of 100 MHz. These pulses are frequency-doubled in a 1 mm long periodically poled Potassium Dihydrogen Phosphate (KDP) crystal cut for type-II second harmonic generation, resulting in 7 mW of 787 nm light. The fundamental 1575 nm light is filtered out with a dichroic mirror and short-pass filter, and the 787 nm beam is focused through 3 μm wide waveguides in a 10 mm long AR-coated KTP crystal, which is periodically poled to phase-match for type-II parametric down-conversion. After the chip, long-pass filters are used to block out the pump light. The horizontally and vertically polarized down-converted photons, centered at 1570 nm and 1580 nm, are split with a polarizing beam splitter cube. The photons are further filtered and coupled into single-mode fibers. The photons at 1570 nm are guided to the client's setup, whereas the photons at 1580 nm are kept the server's side and produce the heralding signal. Alternatively, we use a coherent laser beam at 1550 nm that is attenuated to the single photon level.

These polarization-encoded cobits are sent to the client who implements the required gates using wave plates. We show in the Supplementary Information (SI) that it is sufficient for the client to have access to three half-wave plates (HWP) for the implementation of the NAND gate and to one additional HWP for the implementation of the X^r operation. By applying the following gate sequence:

$$\underbrace{\mathrm{HWP}(\varphi^r)}_{X \text{ or } \mathbf{I}Z} . \underbrace{\mathrm{HWP}(-\theta^{(a\oplus b)}).\mathrm{HWP}(\theta^{-b}).\mathrm{HWP}(\theta^{a})}_{\text{gate implementation}} \quad (4)$$

with $\varphi = \pi/4$ and $\theta = \pi/8$, the client alters the output state, dependent on the values of a and b. The value of the random number r is generated via a classical computer in our implementation. However, this could be easily replaced by a quantum random number generator.

The output cobit is send back to the server who performs a measurement in the computational basis. Experimentally, for both implementations, the polarization of the photons returned to the server is analyzed using a half-wave plate, a Glan-Thompson polarizer and InGaAs avalanche photo diodes that are specified to be 20% efficient and a deadtime set to 10 μs. The results of the server's measurement is then equal to AND(a,b).

Note, that a real physical implementation introduces state-dependent phase shifts, for example $\mathrm{HWP}(0) = \sigma_z$. In order to avoid that these phase shifts reveal any information about a or b, the settings have to be carefully chosen. As we show in the SI, the settings given above are secure in the sense, that these global phase shifts do not reveal any information about our computation. Further, additional phase shifts are introduced when the photons are sent through the fibers. These phase shifts are independent of the settings of a and b and do not affect the correctness of the computation.

RESULTS

We first implement the protocol with single photons. Since the protocol is secure even when multiple photons pass at the same time though the same settings (see SI), a single-shot implementation is not necessary and we integrate the result over 10s of measurement time. In our experiment, we use a Glan-Thompson polarizer and an additional HWP for analysing the

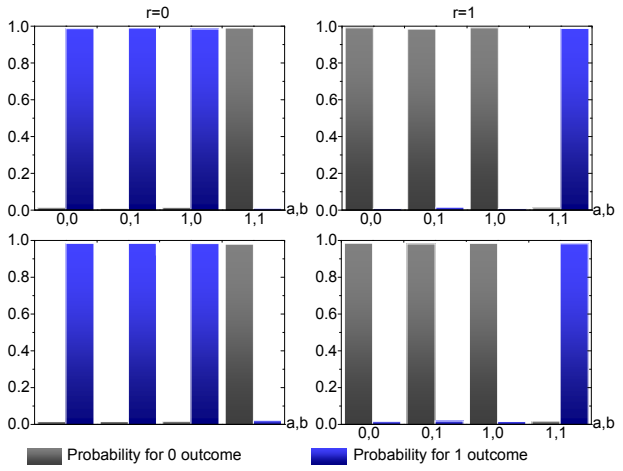

FIG. 4: Results of delegated secure NAND gate. Implementation with single photons (top row) and with an attenuated laser beam (bottom row) for the cases $r = 0$ (left) and $r = 1$ (right). We achieve probabilities for finding the correct output of $(98.8 \pm 0.5)\,\%$ for the single-photon implementation and of $(98.2 \pm 0.06)\,\%$ for the implementation with a coherent beam.

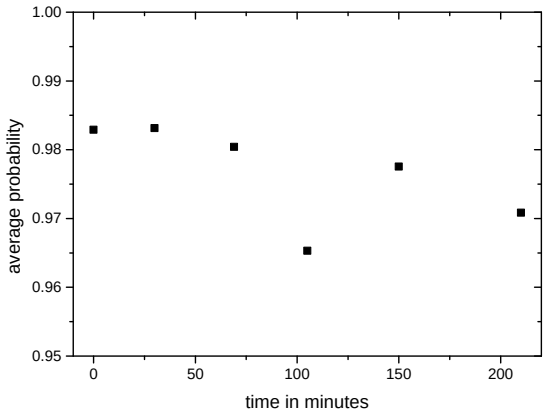

FIG. 5: Study of the long-term stability of our experiment. We repeat the measurement sequence, shown in Fig. 4, six times over 210 minutes and compute the average probability of obtaining the correct result of the NAND computation (averaged over all results, for $r = 0$ and $r = 1$). Error bars are not shown as they are smaller than the symbols.

polarization. The results of the single-photon runs are shown in Fig. 4a. We obtain count rates of 300 heralded photons per second. The average probability for finding the correct results is $(98.8 \pm 0.5)\,\%$.

We run the same experimental sequence with a laser beam that is attenuated to 30000 single counts per second, measured after the transmission through the setup. In this experimental run, we obtain similar average probabilities of finding the correct results of $(98.2 \pm 0.06)\,\%$ (see detailed results in Fig. 4b). In both experiments, the errors are calculated assuming Poissonian errors. Experimental imperfections arise from polarizations drifts when the photons are transmitted through fibers and errors in the manipulations with wave plates as well as imperfection in the measurement in the $|0, 1\rangle$ basis.

The fibres connecting both laboratories are $50\,\mathrm{m}$ long and are placed partly outside the building. In order to test the long-term stability of our fibre connection and influences such as temperature changes and movements of the fibres, we perform a series of NAND-gate measurements for all possible inputs and repeat this measurement six times over 210 minutes. During this period, the obtained probabilities are stable and decrease only slightly from on average $(98.2 \pm 0.06)\,\%$ to $(97.1 \pm 0.08)\,\%$ (see Fig. 5).

CONCLUSION

In this work, we have studied secure delegated computing at the boundary between classical and quantum physics. We have shown that the computational power of classical entity limited to parity computations can be boosted to universal classical computation by exploiting coherence. We have shown that a single qubit can be used as a simple system to accomplish this task—even though no quantumness is required. The extension of previous work to systems capable of being in a coherent superposition of two states provides a practical and robust way to implement the protocol experimentally while still being secure.

We note that the protocol we present here is completely classical in the sense of classical physics. In a different setting, it could also be accomplished with a classical pointer instead of qubits and coherent beams. Here, the classical pointer represents a three-level system, which shows the same functionality than a two-level system with coherence. However, this would also require the client to have a different functionality.

While the focus of our work is more of fundamental nature, demonstrating the computational capability of cobits, a potential practical application of it could be also investigated in future. Note that any partial efficient classical solution for secure cloud computing once boosted to be universal would require a huge overhead. We intend to explore whether our scheme could be used as an alternative scheme where the more costly encoding for NAND computing is done via cobits.

Furthermore, our implementation can be easily extended to long distances using standard technology from quantum key distribution. In the future, it will be interesting to study how this scheme can be extended to multi-party computations, where different parties compute a result while hiding the inputs from each other.

In conclusion, our work shows a new way of how to exploit the properties of both quantum particles and classical fields as tools for classical computing.

ACKNOWLEDGEMENTS

We thank Animesh Datta, Andreas Eckstein, Peter Humphries, Steve Kolthammer, Ben Metcalf, and Josh Nunn for discussions. This work was supported by the Marie Curie Actions within the Seventh Framework Programme for Research of the European Commission, under the Initial Training Network PICQUE, Grant No. 608062 and by the UK Engineering and Physical Sciences Research Council (EPSRC EP/K034480/1).

[1] C. Gentry, in *Proceedings of the 41st annual ACM symposium on Theory of Computing* (ACM, 2009), pp. 169–178.

[2] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* (2009), pp. 517–526.

[3] R. Rivest, L. Adleman, and M. Dertouzos, Foundations of Secure Computation pp. 169–178 (1978).

[4] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[5] T. Morimae, arXiv:1208.1495 (2012).

[6] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).

[7] K. Fisher, A. Broadbent, L. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. Resch, Nature Comm. **5** (2014).

[8] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, arXiv preprint arXiv:1411.5254 (2014).

[9] V. Dunjko, T. Kapourniotis, and E. Kashefi, arXiv preprint arXiv:1405.4558 (2014).

[10] J. Anders and D. E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).

[11] R. Raussendorf and H. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[12] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).

[13] G. Harder, V. Ansari, B. Brecht, T. Dirmeier, C. Marquardt, and C. Silberhorn, Optics Express **21**, 13975 (2013).

Supplementary Information

Correctness of the experimental implementation

The original protocol requires gates to be applied conditioned on the values of a and b [9]. However, when using polarization and wave plates, these might apply state-dependent phase shifts. For example, a half-wave plate (HWP) at "0" setting is equivalent to a σ_Z gate, at a setting of $\pi/8$, it is a Hadamard gate, and at $\pi/4$ it is an σ_X gate. In order to avoid that these state-dependent phase shifts leak information to the server, we need to choose the settings carefully and ensure that the output state contains no information about a and b.

To this end, we choose the following sequence for the implementation of the NAND gate:

$$\mathrm{HWP}(-\theta^{(a\oplus b)}).\mathrm{HWP}(-\theta^{b}).\mathrm{HWP}(\theta^{a})|0\rangle, \qquad (5)$$

with $\theta = \pi/8$. For the settings $a = b = 0$, $a = 0, b = 1$, $a = 1, b = 0$, this gate sequence adds an additional phase shift of π to the state $|1\rangle$. This phase shift can be compensated if we incorporate an additional phase flip in our one-time pad. For this, we use another wave plate $\mathrm{HWP}(\varphi^r)$ with $\varphi = \pi/4$, which allows us to randomly switch between a phase flip and a bit flip. Thus, we can implement the whole scheme using only four HWPs securely:

$$\mathrm{HWP}(\varphi^{r}).\mathrm{HWP}(-\theta^{(a\oplus b)}).\mathrm{HWP}(-\theta^{b}).\mathrm{HWP}(\theta^{a})|0\rangle \qquad (6)$$

with $\varphi = \pi/4$ and $\theta = \pi/8$.

Security of implementation using laser beams

The security of the implemented protocol can follow immediately from the proof given in [9] under two assumptions:

1. ideal devices and or devices with noise/loss, provided the noise/loss parameters are not controlled by the server.

2. the malevolent server does send individual photon states in the modes that ensure the correct operation of the optical elements on the client's side on the polarization degrees of freedom of the photons, e.g. correct frequency of light.

Next we show that the security is not jeopardized under a broader choice of malevolent activity by the server, which can be straightforwardly applied to the coherent light setting.

The cumulative action of optical devices on the client's side are easily seen to implement a polarization rotation of zero degrees, if $\mathrm{NAND}(a, b) \oplus r = 0$, and π otherwise. In other words, the map itself, implemented by the client, is classically one-time padded. Thus, irrespective of the of the actual state prepared by the server, the action of such a map results in a state that is one-time padded by the parameter r, so independent from the client's inputs, when averaged over the client's secret parameter r. The latter means the protocol is blind.

We note that the security may be jeopardized if the server utilizes other modes, e.g. frequency of light, which changes how the optical devices, on the side of the client, manipulate the polarization degrees of freedom. However, such behavior can in principle be prevented by quality control, which sporadically checks the characteristics of light used by the server. More general analyses of how particular implementations may be vulnerable to attacks are beyond the scope of this work.